

EXPONENTIAL COMPLETE RESIDUE SYSTEM

PAOLO LEONETTI

ABSTRACT. This article deals with a question about the existence (and non uniqueness) of a complete residue system in the quotient ring $\mathbb{Z}/n\mathbb{Z}$, where n is a fixed integer greater than 1. In particular it is asked when there exists a permutation σ of the complete residue system $\{1, 2, \dots, n\}$ such that $\{1^{\sigma(1)}, 2^{\sigma(2)}, \dots, n^{\sigma(n)}\}$ is a complete residue system too. The characterization of the set of such integers will be given for almost all n .

1. INTRODUCTION AND NOTATIONS

Given a integer $n \geq 2$, a set of integers $\{a_1, a_2, \dots, a_n\}$ is called a complete residue system if for all integers $i = 1, 2, \dots, n$ there exists a unique $j_i \in \{1, 2, \dots, n\}$ such that n divides $a_{j_i} - i$: in a few words, the set of residues of $\{a_1, a_2, \dots, a_n\}$ modulo n is exactly $\{1, 2, \dots, n\}$. Complete residue systems have an important role in number theory and abstract algebra, e.g. they are related to the complete sets of roots of unity; a concise overview can be found in [9]. A lot of interesting facts about complete residue systems are currently known: here we study a non trivial question about the existence of such set of residues; in particular the answer will be given for almost all integers $n \geq 2$. To be more specific, we first need some notation. We write \mathbb{Z} for the ordered ring of integers, \mathbb{N} for the subsemiring of \mathbb{Z} of nonnegative integers, and \mathbb{N}_0 for $\mathbb{N} \setminus \{0\}$, so that $\mathbb{Z}/n\mathbb{Z}$ represents the quotient ring between \mathbb{Z} and its normal subgroup $n\mathbb{Z}$, i.e. the ring of integers modulo $n \in \mathbb{N}_0$ (see e.g. [8]). Let $\mathbb{P} := \{2, 3, 5, \dots\}$ be the set of all (positive rational) primes; define \mathbb{S} the set of ‘‘Sophie Germain’’ primes, i.e. the subset of \mathbb{P} such that $s \in \mathbb{S}$ if and only if $2s + 1 \in \mathbb{P}$. Here and later, for $m \in \mathbb{Z}$ and $p \in \mathbb{P}$ we use $v_p(m)$ to mean the (standard) p -adic valuation of m , i.e. the greatest $k \in \mathbb{N}$ such that $p^k \mid m$ if m is non zero, otherwise $v_p(0) := \infty$. The arithmetical function $\omega: \mathbb{Z} \rightarrow \mathbb{N} \cup \{\infty\}$ represents the number of distinct prime factors of a non zero integer z , otherwise $\omega(0) := \infty$, and $\text{rad}: \mathbb{Z} \rightarrow \mathbb{N} \cup \{\infty\}$ stands for the radical, the function sending 0 to ∞ and a non-zero integer to the product of its prime divisors; moreover, the Möbius function $\mu: \mathbb{N}_0 \rightarrow \{-1, 0, 1\}$ maps n in $(-1)^{\omega(n)}$ if n is squarefree, otherwise $\mu(n) = 0$. To ease the notation we define also sets $\mathcal{S}_n := \mathbb{Z} \cap [1, n]$ for all $n \in \mathbb{N}_0$. Given two (not necessarily finite) sets $\mathcal{A}_1, \mathcal{A}_2 \subseteq \mathbb{Z}$ and a integer $m \geq 2$, we say that $\mathcal{A}_1 \sim_m \mathcal{A}_2$ if and only if $|\mathcal{A}_1| = |\mathcal{A}_2|$ and there exists a bijective function $f: \mathcal{A}_1 \rightarrow \mathcal{A}_2$ such that $m \mid a - f(a)$ for all $a \in \mathcal{A}_1$. Notice that in particular \sim_m is a equivalence relation, since it’s transitive, and clearly reflexive and symmetric [2]. Observe also that:

$$\mathcal{A}_1 \sim_m \mathcal{A}_2 \quad \text{implies} \quad m \mid \sum_{a_1 \in \mathcal{A}_1} a_1 - \sum_{a_2 \in \mathcal{A}_2} a_2. \quad (1)$$

As usual, we say that $\mathcal{A}_1 \sim \mathcal{A}_2$ if and only if $\mathcal{A}_1 \sim_m \mathcal{A}_2$ for all integers $m \geq 2$, i.e. \mathcal{A}_1 is a permutation of the set \mathcal{A}_2 ; finally, given integers α, β and a set $\mathcal{A} \subseteq \mathbb{Z}$, then $(\alpha\mathcal{A} + \beta) := \{z \in \mathbb{Z} : z = \alpha a + \beta \text{ for some } a \in \mathcal{A}\}$. For notation and terminology used but not defined here, as well as for material concerning classical topics in number theory, the reader should refer to [5].

2. MAIN QUESTION

A integer $n \geq 2$ is defined ‘‘exponential’’ if and only if there exists a function $\sigma: \mathcal{S}_n \rightarrow \mathcal{S}_n$ such that

$$\{\sigma(1), \sigma(2), \dots, \sigma(n)\} \sim \mathcal{S}_n \quad \text{and} \quad \{1^{\sigma(1)}, 2^{\sigma(2)}, \dots, n^{\sigma(n)}\} \sim_n \mathcal{S}_n.$$

Notice that, according to definition of section 1, a set \mathcal{A} of integers is a complete residue system in $\mathbb{Z}/n\mathbb{Z}$ if and only if $\mathcal{A} \sim_n \mathcal{S}_n$. Having this in mind, we can state the basic question addressed by the article:

Conjecture. A integer $n \geq 2$ is exponential if and only if $n2^{-v_2(n)} \in (2\mathbb{S} + 1) \cup \{1, 3\}$ and $v_2(n) \leq 1$.

Although the article does not present a whole solution of the above Conjecture, the latter has been proved for almost all integers n : more precisely, if \mathbb{M} is the set of integer $n \geq 2$ such that the conjecture does not hold and x is sufficiently large, then

$$|\mathbb{M} \cap [1, x]| = \mathcal{O}\left(\frac{x}{\ln x}\right), \quad (2)$$

where \mathcal{O} is the Bachmann-Landau symbol (see e.g. [6]), i.e. there exists a positive constant K such that $|\mathbb{M} \cap [1, x]| \leq Kx/\ln x$ for all $x \geq 2$; in particular we will see that if x is sufficiently large then $K = \frac{1}{5}$ works. Two theorems are going to be proved: the first one studies the case n odd, the second one the case n even.

Theorem 1. *A integer $n \geq 2$ such that $v_2(n) = 0$ is exponential if and only if $n \in (2\mathbb{S} + 1) \cup \{3\}$.*

Notice that Theorem 1 states that, equivalently, no odd counterexamples exists, i.e. $\mathbb{M} \cap (2\mathbb{N} + 1) = \emptyset$.

Theorem 2. *A integer $n \geq 2$ such that $v_2(n) \geq 1$ is exponential only if $n = 2$ or if $\frac{1}{2}n \in \mathbb{P}$ such that $\mu^2(\frac{1}{2}n - 1) = 1$. Moreover, if a integer $n \geq 2$ such that $v_2(n) = 1$ verifies $\frac{1}{2}n \in (2\mathbb{S} + 1) \cup \{1, 3\}$, then n is exponential.*

Section 3 shows preliminary facts that hold independently of the parity of n ; Theorems 1 and 2 are proved in Sections 4 and 5. Finally, conclusions follow in Section 6.

3. PRELIMINARIES

Notice all integers n such that $2 \leq n \leq 7$ are exponential (i.e. $\mathbb{M} \cap [2, 7] = \emptyset$), indeed it's enough to choose

| | $\sigma(1)$ | $\sigma(2)$ | $\sigma(3)$ | $\sigma(4)$ | $\sigma(5)$ | $\sigma(6)$ | $\sigma(7)$ |
|---------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|
| $n = 2$ | 1 | 2 | ★ | ★ | ★ | ★ | ★ |
| $n = 3$ | 2 | 1 | 3 | ★ | ★ | ★ | ★ |
| $n = 4$ | 2 | 1 | 3 | 4 | ★ | ★ | ★ |
| $n = 5$ | 2 | 5 | 1 | 3 | 4 | ★ | ★ |
| $n = 6$ | 2 | 1 | 4 | 5 | 3 | 6 | ★ |
| $n = 7$ | 6 | 2 | 1 | 5 | 7 | 3 | 4 |

From now on, let's suppose $n \geq 8$; for any such integer n define the set $\mathcal{A}_n := \{z \in \mathbb{Z} : \text{rad}(n) \mid z\} \cap [1, n-1]$ so that we easily have $|\mathcal{A}_n| = \frac{n}{\text{rad}(n)} - 1$. Notice also working in $\mathbb{Z}/n\mathbb{Z}$ that $a \in \mathcal{A}_n$ implies $a^{\sigma(a)} \in \mathcal{A}_n$ and $n \mid n^{\sigma(n)}$ whatever $\sigma(n) \in \mathcal{S}_n$ is. But $\{1^{\sigma(1)}, 2^{\sigma(2)}, \dots, n^{\sigma(n)}\}$ need to be a complete residue system in $\mathbb{Z}/n\mathbb{Z}$, so that $n \nmid a^{\sigma(a)}$, for all $a \in \mathcal{A}_n$. In particular, since $a \in \mathcal{A}_n$ implies $\text{rad}(n) \mid a$, we have also:

$$n \nmid \text{rad}(n)^{\sigma(a)}, \text{ for all } a \in \mathcal{A}_n. \quad (3)$$

But $\{\sigma(1), \sigma(2), \dots, \sigma(n)\}$ is another permutation of \mathcal{S}_n , so that relation (3) holds for at least $|\mathcal{A}_n|$ distinct positive integers. In particular it implies that $n \nmid \text{rad}(n)^{|\mathcal{A}_n|}$. It means that there exists a prime $p \in \mathbb{P}$ such that $p \mid n$ and

$$v_p(n) \geq |\mathcal{A}_n| + 1 = p^{v_p(n)-1} \left(\prod_{q \in \mathbb{P} \setminus \{p\} \text{ such that } q \mid n} q^{v_q(n)-1} \right) \geq p^{v_p(n)-1}. \quad (4)$$

Inequality (4) implies that:

- ◇ if $p = 2$ then $v_2(n) = 1$ or $v_2(n) = 2$, and $v_q(n) = 1$ for all other primes q that divide n ;
- ◇ if $p \geq 3$ then $v_p(n) = 1$, and $v_q(n) = 1$ for all other primes q that divide n (i.e. n is squarefree).

To sum up, if such a integer $n \geq 8$ is exponential, then $n = r$ or $n = 2r$ or $n = 4r$, where r denotes some odd squarefree integer greater than 1, i.e. $\mu^2(n2^{-v_2(n)}) = 1$ and $v_2(n) \leq 2$.

Define now \mathcal{Q}_n the set of quadratic residues of $\mathbb{Z}/n\mathbb{Z}$, i.e. $\mathcal{Q}_n := \{z \in \mathcal{S}_n : n \mid s^2 - z \text{ for some } s \in \mathcal{S}_n\}$. Since $|\mathcal{Q}_n|$ has to be also the number of quadratic residues of $\{1^{\sigma(1)}, 2^{\sigma(2)}, \dots, n^{\sigma(n)}\}$ in $\mathbb{Z}/n\mathbb{Z}$ and at least $\lfloor \frac{1}{2}n \rfloor$ numbers in \mathcal{S}_n are even, then

$$|\mathcal{Q}_n| \geq \left\lfloor \frac{1}{2}n \right\rfloor. \quad (5)$$

On the one hand if a integer $z \in \mathcal{Q}_n$ is chosen, then $z \in \mathcal{Q}_m$ too, for all $m \in \mathbb{N}_0$ such that $m \mid n$; on the other hand, if $z_1 \in \mathcal{Q}_{m_1}$ and $z_2 \in \mathcal{Q}_{m_2}$ for some distinct and coprime integers $m_1, m_2 \in \mathbb{N}_0$, then by Chinese remainder theorem [5] there exists a unique $z_3 \in \mathcal{Q}_{m_1 m_2}$ such that $m_1 \mid z_3 - z_1$ and $m_2 \mid z_3 - z_2$: in other words, the function $n \mapsto |\mathcal{Q}_n|$ is multiplicative.

3.1. **Case** $v_2(n) = 2$. If a integer $n \geq 8$ is exponential and $v_2(n) = 2$ then $n = 4r$ where $r := \prod_{i=1}^{\omega(r)} q_i$ represents a odd squarefree integer greater than 1, and $q_1, q_2, \dots, q_{\omega(r)}$ are distinct odd primes of \mathbb{P} . Then inequality (5) implies

$$|\mathcal{Q}_4| \prod_{i=1}^{\omega(r)} |\mathcal{Q}_{q_i}| = |\mathcal{Q}_n| \geq \left\lfloor \frac{1}{2}n \right\rfloor = 2 \prod_{i=1}^{\omega(r)} q_i. \quad (6)$$

Since it's well-known that $|\mathcal{Q}_4| = 2$ and $|\mathcal{Q}_{q_i}| = \frac{1}{2}(q_i + 1)$, inequality (6) is equivalent to

$$\prod_{i=1}^{\omega(r)} \left(\frac{1}{2} + \frac{1}{2q_i} \right) \geq 1,$$

that is false for all squarefree odd integers $r \geq 3$.

3.2. **Case** $v_2(n) = 1$. If a integer $n \geq 8$ is exponential and $v_2(n) = 1$ then $n = 2r$ where $r := \prod_{i=1}^{\omega(r)} q_i$ represents a odd squarefree integer greater than 1, and $q_1, q_2, \dots, q_{\omega(r)}$ are distinct odd primes of \mathbb{P} . Then inequality (5) implies

$$|\mathcal{Q}_2| \prod_{i=1}^{\omega(r)} |\mathcal{Q}_{q_i}| = |\mathcal{Q}_n| \geq \left\lfloor \frac{1}{2}n \right\rfloor = \prod_{i=1}^{\omega(r)} q_i. \quad (7)$$

Since it's well-known that $|\mathcal{Q}_2| = 2$ and $|\mathcal{Q}_{q_i}| = \frac{1}{2}(q_i + 1)$, inequality (7) is equivalent to

$$\prod_{i=1}^{\omega(r)} \left(\frac{1}{2} + \frac{1}{2q_i} \right) \geq \frac{1}{2}. \quad (8)$$

But if $\omega(r) \geq 2$ then also the following chain of inequalities holds true:

$$\prod_{i=1}^{\omega(r)} \left(\frac{1}{2} + \frac{1}{2q_i} \right) \leq \prod_{i=1}^{\omega(r)} \left(\frac{1}{2} + \frac{1}{2 \cdot 3} \right) = \left(\frac{2}{3} \right)^{\omega(r)} \leq \frac{4}{9}$$

contradicting inequality (8). Moreover, if $\omega(r) = 1$ then inequality (8) is trivially verified: it means that if a integer $n \geq 8$ such that $v_2(n) = 1$ is exponential then $\frac{1}{2}n \in \mathbb{P}$.

3.3. **Case** $v_2(n) = 0$. If a integer $n \geq 8$ is exponential the statement and $2 \nmid n$ then $n = r$ where $r := \prod_{i=1}^{\omega(r)} q_i$ represents a odd squarefree integer greater than 1, and $q_1, q_2, \dots, q_{\omega(r)}$ are distinct odd primes of \mathbb{P} . Then inequality (5) implies

$$\prod_{i=1}^{\omega(r)} |\mathcal{Q}_{q_i}| = |\mathcal{Q}_n| \geq \left\lfloor \frac{1}{2}n \right\rfloor = \frac{1}{2} \left(-1 + \prod_{i=1}^{\omega(r)} q_i \right). \quad (9)$$

As before, we can rewrite inequality (9) in the equivalent form

$$2^{1-\omega(r)} \prod_{i=1}^{\omega(r)} \left(1 + \frac{1}{q_i} \right) \geq 1 - \frac{1}{r}. \quad (10)$$

But if $\omega(r) \geq 2$ then also the following chain of inequalities holds true:

$$2^{1-\omega(r)} \prod_{i=1}^{\omega(r)} \left(1 + \frac{1}{q_i} \right) \leq 2^{1-\omega(r)} \cdot \frac{4}{3} \cdot \left(\frac{6}{5} \right)^{\omega(r)-1} = \frac{4}{3} \left(\frac{3}{5} \right)^{\omega(r)-1} \leq \frac{4}{5},$$

contradicting inequality (10) in case $r \geq 6$. Moreover, if $\omega(r) = 1$ then inequality (10) trivially holds: it means that if a odd integer $n \geq 8$ is exponential then $n \in \mathbb{P}$.

4. PROOF OF THEOREM 1

According to what we said in Section 3, if $2 \nmid n$ we can assume that there exists a prime $p \in \mathbb{P}$ such that $n = p$ and $p \geq 11$. The proof of Theorem 1 is divided into five parts: in particular subsections 4.1, 4.2 and 4.3 are not strictly essential, but they are just interesting exercises that give an idea on how the construction of subsection 4.5 has been thought.

4.1. About $\sigma(p)$. We claim that $\sigma(p) \notin \{1, p\}$. Suppose the contrary, then $\{\sigma(1), \sigma(2), \dots, \sigma(p-1)\} \sim_{p-1} \mathcal{S}_{p-1}$; define $g \in \mathcal{S}_p$ one of the $\varphi(\varphi(p))$ primitive roots of $(\mathbb{Z}/p\mathbb{Z})^*$ (see [5] for a proof of the existence of such a primitive root) where, as usual, φ represents the Euler indicator. Then we can find integers $\alpha_1, \beta_1, \alpha_2, \beta_2, \dots, \alpha_{p-1}, \beta_{p-1}$ such that $\{\alpha_1, \alpha_2, \dots, \alpha_{p-1}\} \sim \{\beta_1, \beta_2, \dots, \beta_{p-1}\} \sim \mathcal{S}_{p-1}, p \mid z - g^{g^{\alpha_z}}$ for all $z \in \mathcal{S}_{p-1}$, i.e. $\{g^{g^{\alpha_1}}, g^{g^{\alpha_2}}, \dots, g^{g^{\alpha_{p-1}}}\} \sim_p \mathcal{S}_{p-1}$ and $p \mid \sigma(z) - g^{\beta_z}$ for all $z \in \mathcal{S}_{p-1}$, i.e. $\{g^{\beta_1}, g^{\beta_2}, \dots, g^{\beta_{p-1}}\} \sim_p \mathcal{S}_{p-1}$. It implies that

$$\{g^{g^{\alpha_1+\beta_1}}, g^{g^{\alpha_2+\beta_2}}, \dots, g^{g^{\alpha_{p-1}+\beta_{p-1}}}\} \sim_p \mathcal{S}_{p-1},$$

that is equivalent to $\{\alpha_1 + \beta_1, \alpha_2 + \beta_2, \dots, \alpha_{p-1} + \beta_{p-1}\} \sim_{p-1} \mathcal{S}_{p-1}$. By assumption we have also that $\{\beta_1, \beta_2, \dots, \beta_{p-1}\} \sim_{p-1} \mathcal{S}_{p-1}$. For \sim_m is an equivalence relation, we have also $\{\alpha_1 + \beta_1, \alpha_2 + \beta_2, \dots, \alpha_{p-1} + \beta_{p-1}\} \sim_{p-1} \{\beta_1, \beta_2, \dots, \beta_{p-1}\}$. Applying (1) the following divisibility holds

$$p-1 \mid \sum_{i \in \mathcal{S}_{p-1}} (\alpha_i + \beta_i) - \sum_{i \in \mathcal{S}_{p-1}} \beta_i = \sum_{i \in \mathcal{S}_{p-1}} \alpha_i.$$

But by construction $\{\alpha_1, \alpha_2, \dots, \alpha_{p-1}\} \sim \mathcal{S}_{p-1}$, so that it simplifies to $p-1 \mid \sum_{i \in \mathcal{S}_{p-1}} \alpha_i = \sum_{i \in \mathcal{S}_{p-1}} i = \frac{1}{2}p(p-1)$, that is impossible in $\mathbb{Z}/2^{v_2(p-1)}\mathbb{Z}$.

4.2. About $\sigma^{-1}(p-1)$. Since $p \mid z^p - z = 0$ for all $p \in \mathbb{P}$ and $z \in \mathbb{Z}$ (Fermat's little theorem [5]), we must have $p-1 \in \{\sigma(1), \sigma(p)\}$. Notice also that if a prime p is exponential with permutation $\{\sigma(1), \sigma(2), \sigma(3), \dots, \sigma(p-1), \sigma(p)\} \sim \mathcal{S}_p$, then the permutation $\{\sigma(p), \sigma(2), \sigma(3), \dots, \sigma(p-1), \sigma(1)\} \sim \mathcal{S}_p$ works too, i.e. we can assume without loss of generality that $\sigma(1) = p-1$.

4.3. About $\sigma^{-1}(\frac{1}{2}(p-1))$. According to notation of Section 3, we have $\mathcal{Q}_p \sim_p \{g^2, g^4, \dots, g^{p-1}, p\}$ so that in particular $|\mathcal{Q}_p| = \frac{1}{2}(p+1)$. Moreover, if $z \in \mathcal{S}_p$ then $z^{\sigma(z)}$ is a quadratic residues whenever $2 \mid \sigma(z)$. It implies that $\{\sigma(g^2), \sigma(g^4), \dots, \sigma(g^{p-1}), \sigma(p)\} \sim \{2, 4, \dots, p-1, v\}$ for some $v \in \mathcal{S}_p \cap 2\mathbb{N} + 1$. If $4 \mid p-1$ then $p-1 = (g^{\frac{p-1}{4}})^2$ in $\mathbb{Z}/p\mathbb{Z}$, i.e. $p-1 \in \mathcal{Q}_p$; but $1^{\sigma(1)} = 1$ whatever $\sigma(1) \in \mathcal{S}_p$ is, implying that $\sigma(p-1) = v$. Also, it's well known that for all integers z not divisible by p we have $z^{\frac{p-1}{2}} = \left(\frac{z}{p}\right) \in \{1, -1\}$ in $\mathbb{Z}/p\mathbb{Z}$, where $\left(\frac{z}{p}\right)$ represents the Legendre symbol, implying that:

- ◇ If $4 \mid p+1$ then $\frac{1}{2}(p-1) \in \{\sigma(1), \sigma(p-1), \sigma(p)\}$.
- ◇ If $4 \mid p-1$ then $\frac{1}{2}(p-1) \in \{\sigma(1), \sigma(p)\}$.

4.4. About $\mu^2(p-1)$. We claim that $p-1$ is squarefree. Let's suppose the contrary, i.e. there exists a prime $q \in \mathbb{P}$ such that $v_q(p-1) \geq 2$. For all $m, n \in \mathbb{N}_0$ define $\mathcal{P}_{n,m}$ the set of m -powers in $\mathbb{Z}/n\mathbb{Z}$, i.e.

$$\mathcal{P}_{n,m} := \{z \in \mathcal{S}_n : n \mid s^m - z \text{ for some } s \in \mathcal{S}_n\},$$

so that in particular $\mathcal{P}_{n,2} \sim \mathcal{Q}_n$. It's straightforward to verify that in our case $|\mathcal{P}_{p,m}| = \frac{p-1}{\gcd(p-1,m)} + 1$; in particular $|\mathcal{P}_{p,q}| = \frac{p-1}{q} + 1$ and $|\mathcal{P}_{p,q^2}| = \frac{p-1}{q^2} + 1$. Define also $\mathcal{M}_{n,m}$ the set of positive integers multiple of m and smaller than n , i.e.

$$\mathcal{M}_{n,m} := \{z \in \mathcal{S}_{n-1} : m \mid z\}.$$

It's clear that $|\mathcal{M}_{n,m}| = \lfloor \frac{n-1}{m} \rfloor$ so that in particular $|\mathcal{M}_{p,q}| = \frac{p-1}{q}$ and $|\mathcal{M}_{p,q^2}| = \frac{p-1}{q^2}$. Observe now that:

- ◇ If $z \in \mathcal{P}_{p,q}$ then $z^{\sigma(z)}$ is a q -th power too, whatever $\sigma(z) \in \mathcal{S}_p$ is;
- ◇ If $\sigma(z) \in \mathcal{M}_{p,q}$ then $z^{\sigma(z)}$ is a q -th power, whatever $z \in \mathcal{S}_p$ is;
- ◇ $|\mathcal{M}_{p,q}| < |\mathcal{P}_{p,q}|$.

Since the numbers of q -powers in $\mathbb{Z}/p\mathbb{Z}$ of the sets $\{1^{\sigma(1)}, 2^{\sigma(2)}, \dots, p^{\sigma(p)}\} \sim_p \{1, 2, \dots, p\}$ have to be equal, we can deduce that $\sigma(z) \in \mathcal{M}_{p,q}$ implies $z \in \mathcal{P}_{p,q}$, and in particular (the residue of) $z^{\sigma(z)}$ belongs to \mathcal{P}_{p,q^2} . It means that $|\mathcal{M}_{p,q}| \leq |\mathcal{P}_{p,q^2}|$, i.e. $\frac{p-1}{q} \leq 1 + \frac{p-1}{q^2} \leq 1 + \frac{p-1}{2q}$, implying that $q \geq \frac{1}{2}(p-1)$. At the same time $q^2 \mid p-1$, so that $q \leq \sqrt{p-1}$, and in particular $\frac{1}{2}(p-1) \leq \sqrt{p-1}$ that is false for all primes $p \geq 7$. We concluded that if $n \in \mathbb{P}$ is exponential then $\mu^2(n-1) = 1$, i.e. $n-1$ is squarefree.

4.5. A necessary condition (I). Since $p \geq 11$ and $p-1$ is a even squarefree, so that $\omega(p-1) \geq 2$, we can find primes $2 = q_1 < q_2 < \dots < q_{\omega(p-1)}$ such that $p = 1 + \prod_{i=1}^{\omega(p-1)} q_i$. We claim that $\omega(p-1) = 2$, i.e. $\frac{1}{2}(p-1) \in \mathbb{S}$. Let's suppose the contrary, viz. $\omega(p-1) \geq 3$, so that $2 \nmid q_{\omega(p-1)-1} q_{\omega(p-1)}$. Define the integers $\gamma_1 := (p-1)/q_{\omega(p-1)-1}$ and $\gamma_2 := (p-1)/q_{\omega(p-1)}$, noticing that $2 \mid \gcd(\gamma_1, \gamma_2)$. Then at least one between $\gamma_1 \nmid \sigma(p)$ and $\gamma_2 \nmid \sigma(p)$ holds: indeed, if it's not the case then $p-1 = \text{lcm}(\gamma_1, \gamma_2) \mid \sigma(p)$; together with $\sigma(p) \in \mathcal{S}_p$ it implies $\sigma(p) = p-1$. But we already assumed without loss of generality that $\sigma(1) = p-1$ in subsection 4.2, and that's a contradiction. So it's well defined a integer $\gamma \in \{\gamma_1, \gamma_2\}$ such that $\gamma \nmid \sigma(p)$. Moreover $\mathcal{P}_{p,\gamma} \sim_p \{g^\gamma, g^{2\gamma}, \dots, g^{p-1}, p\}$, so that $|\mathcal{P}_{p,\gamma}| = \frac{p-1}{\gamma} + 1$ and $\sigma(p) \notin \{\gamma, 2\gamma, \dots, p-1\} = \mathcal{M}_{p,\gamma}$, that $|\mathcal{M}_{p,\gamma}| = \frac{p-1}{\gamma}$. Now, if $z \in \mathcal{S}_p$ and $\sigma(z) \in \mathcal{M}_{p,\gamma}$ then $z^{\sigma(z)}$ is a γ -power in $\mathbb{Z}/p\mathbb{Z}$: it means that there exists a permutation $\{\tilde{\sigma}(\gamma), \tilde{\sigma}(2\gamma), \dots, \tilde{\sigma}(p-1)\} \sim \mathcal{M}_{p,\gamma}$ such that

$$\{g^{\gamma\tilde{\sigma}(\gamma)}, g^{2\gamma\tilde{\sigma}(2\gamma)}, \dots, g^{(p-1)\tilde{\sigma}(p-1)}\} \sim_p \{g^\gamma, g^{2\gamma}, \dots, g^{p-1}\} \quad (11)$$

Notice then that we have to have by force $\tilde{\sigma}(p-1) = p-1$: indeed if $\tilde{\sigma}(i_0\gamma) = p-1$ for some $i_0 \in \mathcal{S}_{\frac{p-1}{\gamma}-1}$ then

$$p \mid \gcd\left(g^{(p-1)\tilde{\sigma}(p-1)} - 1, g^{i_0\gamma\tilde{\sigma}(i_0\gamma)} - 1\right)$$

whatever $\tilde{\sigma}(p-1) \in \mathcal{S}_p$ is. It implies that (11) simplifies to

$$\{g^{\gamma\tilde{\sigma}(\gamma)}, g^{2\gamma\tilde{\sigma}(2\gamma)}, \dots, g^{(p-1-\gamma)\tilde{\sigma}(p-1-\gamma)}\} \sim_p \{g^\gamma, g^{2\gamma}, \dots, g^{p-1-\gamma}\},$$

that is equivalent to

$$\{\gamma\tilde{\sigma}(\gamma), 2\gamma\tilde{\sigma}(2\gamma), (p-1-\gamma)\tilde{\sigma}(p-1-\gamma)\} \sim_{p-1} \{\gamma, 2\gamma, \dots, p-1-\gamma\}. \quad (12)$$

Since each integer is divisible by γ in both sets and by construction $\frac{p-1}{\gamma} \in \{q_{\omega(p-1)-1}, q_{\omega(p-1)}\}$ is a odd prime, then (12) implies that

$$\left\{\tilde{\sigma}(\gamma), 2\tilde{\sigma}(2\gamma), \dots, \left(\frac{p-1}{\gamma} - 1\right)\tilde{\sigma}\left(\left(\frac{p-1}{\gamma} - 1\right)\gamma\right)\right\} \sim_{\frac{p-1}{\gamma}} \left\{1, 2, \dots, \frac{p-1}{\gamma} - 1\right\}$$

In particular, the product of all elements of each set must be the same in the quotient ring $\mathbb{Z}/\frac{p-1}{\gamma}\mathbb{Z}$: on the one hand, once we observe that $\gcd(\gamma, \frac{p-1}{\gamma}) = 1$, the product of elements of the first set is

$$\left(\frac{p-1}{\gamma} - 1\right)! \prod_{i \in \mathcal{S}_{\frac{p-1}{\gamma}-1}} \tilde{\sigma}(i\gamma) = \left(\frac{p-1}{\gamma} - 1\right)! 2^{\frac{p-1}{\gamma}-1} = 1$$

in $\mathbb{Z}/\frac{p-1}{\gamma}\mathbb{Z}$, thanks to Wilson theorem and Fermat's little theorem [5]; on the another hand the product of elements of the second set is

$$\left(\frac{p-1}{\gamma} - 1\right)! = -1.$$

That's a contradiction, since $\frac{p-1}{\gamma} \geq 3$. Hence, if $n = p \in \mathbb{P}$ is exponential then $\frac{1}{2}(p-1)$ is prime too, i.e. $\frac{1}{2}(p-1) \in \mathbb{S}$.

4.6. A sufficient condition (I). We claim that if $\ell \in \mathbb{S}$ then $p := 2\ell + 1$ is exponential. Having in mind results from subsections 4.1, 4.2 and 4.3, let's start to construct the solution setting at first $\sigma(1) = 2\ell$, $\sigma(2\ell) = \ell$ and $\sigma(2\ell+1) = \ell+1$. Define g a generator of $(\mathbb{Z}/p\mathbb{Z})^*$, and q a generator of $(\mathbb{Z}/2\ell\mathbb{Z})^*$; in particular they exist and $2 \nmid q$. Define finally the sets:

- ◊ $\mathfrak{Q} \subset \mathcal{S}_p$ such that $\mathfrak{Q} \sim_p \{g^{(2q)^1}, g^{(2q)^2}, \dots, g^{(2q)^{\ell-1}}\}$, i.e. all quadratic residues except 0 and 1;
- ◊ $\mathfrak{N} \subset \mathcal{S}_p$ such that $\mathfrak{N} \sim_p \{g^{q^0}, g^{q^1}, \dots, g^{q^{\ell-2}}\}$, i.e. all other residues except 2ℓ ;
- ◊ $\mathcal{E} \subset \mathcal{S}_p$ such that $\mathcal{E} \sim_{p-1} \{(2q)^1, (2q)^2, \dots, (2q)^{\ell-2}\} \cup \{q^{\frac{\ell-1}{2}}\}$, i.e. all even integers in \mathcal{S}_p except 2ℓ and $\ell+1$, and adding $2\ell-1$;
- ◊ $\mathcal{O} \subset \mathcal{S}_p$ such that $\mathcal{O} \sim_{p-1} \{q^0, q^0, q^1, q^2, \dots, q^{\ell-2}\} \setminus \{q^{\frac{\ell-1}{2}}\}$, i.e. all odd integers in \mathcal{S}_p except ℓ and $2\ell-1$ (here for simplicity the first two elements represents 1 and p).

In particular, notice that $|\mathfrak{Q}| = |\mathfrak{N}| = |\mathcal{E}| = |\mathcal{O}| = \ell-1$.

Then it's enough to set

$$\diamond \sigma(g^{q^i}) = q^i \text{ for all } i = 0, 1, 2, \dots, \frac{\ell-3}{2};$$

$$\diamond \sigma \left(g^{q^i} \right) = q^{i+1} \text{ for all } i = \frac{\ell-1}{2}, \frac{\ell+1}{2}, \dots, \ell-2;$$

and

$$\begin{aligned} \diamond \sigma \left(g^{(2q)^i} \right) &= (2q)^i \text{ for all } i = 1, 2, \dots, \frac{\ell-1}{2}; \\ \diamond \sigma \left(g^{(2q)^i} \right) &= (2q)^{i-1} \text{ for all } i = \frac{\ell+1}{2}, \frac{\ell+3}{2}, \dots, \ell-2; \\ \diamond \sigma \left(g^{(2q)^{\ell-1}} \right) &= (2q)^{\ell-2}. \end{aligned}$$

To verify that this construction really works, one can easily check that

$$\begin{aligned} \diamond g^{q^i} \text{ for all } i = 0, 1, 2, \dots, \frac{\ell-3}{2} \text{ and } g^{q^i} \text{ for all } i = \frac{\ell-1}{2}, \frac{\ell+1}{2}, \dots, \ell-2 \text{ represents in } \mathbb{Z}/p\mathbb{Z} \text{ the whole set } \mathfrak{N}; \\ \diamond q^i \text{ for all } i = 1, 2, \dots, \frac{\ell-1}{2} \text{ and } q^{i+1} \text{ for all } i = \frac{\ell-1}{2}, \frac{\ell+1}{2}, \dots, \ell-2 \text{ represents in } \mathbb{Z}/p\mathbb{Z} \text{ the whole set } \mathcal{O}; \\ \diamond g^{q^i \sigma(g^{q^i})} \text{ for all } i = 0, 1, 2, \dots, \ell-2 \text{ represents in } \mathbb{Z}/p\mathbb{Z} \text{ the whole set } \mathfrak{N}; \end{aligned}$$

and

$$\begin{aligned} \diamond g^{(2q)^i} \text{ for all } i = 1, 2, \dots, \ell-1 \text{ represents in } \mathbb{Z}/p\mathbb{Z} \text{ the whole set } \mathfrak{Q}; \\ \diamond (2q)^i \text{ for all } i = 1, 2, \dots, \frac{\ell-1}{2} \text{ and } (2q)^{i-1} \text{ for all } i = \frac{\ell+1}{2}, \frac{\ell+3}{2}, \dots, \ell-2, \text{ adding } (2q)^{\ell-2}, \text{ represents in } \\ \mathbb{Z}/p\mathbb{Z} \text{ the whole set } \mathcal{E}; \\ \diamond g^{(2q)^i \sigma(g^{(2q)^i})} \text{ for all } i = 1, 2, \dots, \ell-1 \text{ represents in } \mathbb{Z}/p\mathbb{Z} \text{ the whole set } \mathfrak{Q}. \end{aligned}$$

5. PROOF OF THEOREM 2

5.1. A necessary condition (II). According to what we said in Section 3, if a even integer $n \geq 2$ is exponential then there exists a prime $p \in \mathbb{P}$ such that $n = 2p$ with $p \geq 5$. Observe that $|\mathcal{P}_{2p,m}| = 2|\mathcal{P}_{p,m}|$ for all positive integer m . Indeed, on the one hand if $z \in \mathcal{P}_{p,m}$ then $\{z, z+p\} \subset \mathcal{P}_{2p,m}$; on the other hand, if $z \in \mathcal{P}_{2p,m}$ then its residue in $\mathbb{Z}/p\mathbb{Z}$ belongs to $\mathcal{P}_{p,m}$. Once defined $\mathcal{X} := \{1, p, p+1, 2p\}$, we have that $2p \mid x^{\sigma(x)} - x$ for all $x \in \mathcal{X}$ and $\sigma(x) \in \mathcal{S}_{2p}$, implying that $2 \nmid \sigma(p-1)\sigma(2p-1)$. Suppose that $4 \mid p-1$. Since $\left(\frac{-1}{p}\right) = 1$ then $\{p-1, 2p-1\} \subset \mathcal{P}_{2p,2}$. But the number of even numbers in \mathcal{S}_{2p} is strictly less than $|\mathcal{P}_{2p,2}|$, i.e. $p = |\mathcal{M}_{2p+1,2}| < |\mathcal{P}_{2p,2}| = p+1$. In particular if a integer $\sigma(z) \in \mathcal{M}_{2p+1,2}$ then $z \in \mathcal{P}_{2p,2}$, otherwise the set $\{1^{\sigma(1)}, 2^{\sigma(2)}, \dots, (2p)^{\sigma(2p)}\}$ will have (stricly) more than $p+1$ quadratic residues in $\mathbb{Z}/2p\mathbb{Z}$. But that's in contradiction with $\{p-1, 2p-1\} \subset \mathcal{P}_{2p,2}$ and $2 \nmid \sigma(p-1)\sigma(2p-1)$: indeed also the following inequality should work too $|\mathcal{P}_{2p,2}| - |\mathcal{M}_{2p+1,2}| \geq 2$. Hence, if a even integer $n \geq 8$ is exponential, then $n = 2p$ for some prime p and $v_2(p-1) = 1$.

Corollary: $n = 10$ is not exponential.

That's why from now on we can assume $p \geq 7$. We claim that $\mu^2(p-1) = 1$, i.e. $p-1$ has to be squarefree; suppose the contrary, i.e. there exists a (odd) prime $q \in \mathbb{P}$ such that $v_q(p-1) \geq 2$. Then, reasoning as in Section 4, we need to have $|\mathcal{P}_{2p,q^2}| \geq |\mathcal{M}_{2p+1,q}|$. Since $q \mid q^2 \mid p-1 \mid 2(p-1)$, then $|\mathcal{M}_{2p+1,q}| \geq 2|\mathcal{M}_{p,q}|$, implying that $2|\mathcal{M}_{p,q}| \leq |\mathcal{M}_{2p+1,q}| \leq |\mathcal{P}_{2p,q^2}| = 2|\mathcal{P}_{p,q^2}|$. But we already proved in subsection 4.4 that the inequality $|\mathcal{M}_{p,q}| \leq |\mathcal{P}_{p,q^2}|$ has no solutions, whenever $p \geq 7$.

5.2. A sufficient condition (II). We claim that if $\ell \in \mathbb{S}$ then $2(2\ell+1)$ is exponential. To make a similar notation of subsection 4.6 we define $p := 2\ell+1$, g a generator of $(\mathbb{Z}/2p\mathbb{Z})^*$, and q a generator of $(\mathbb{Z}/2\ell\mathbb{Z})^*$; in particular they exist and $2 \nmid gq$. As suggested in subsection 5.1 let's begin fixing values of \mathcal{X} : $\sigma(1) = p-1$, $\sigma(p) = 2p-1$, $\sigma(p+1) = 2p-2$ and $\sigma(2p) = 2p$. Moreover, we set $\sigma(g^\ell) = \frac{1}{2}(p-1)$ and $\sigma((2g)^\ell) = \frac{3}{2}(p-1)$. Since in $\mathbb{Z}/2\mathbb{Z}$ trivially $z^{\sigma(z)} = z$ for all $z \in \mathcal{S}_{2p}$ and $\sigma(z) \in \mathcal{S}_{2p}$, it's enough to consider the set \mathcal{S}_{2p} in $\mathbb{Z}/p\mathbb{Z}$ and the set of exponents in $\mathbb{Z}/(p-1)\mathbb{Z}$. Following this observation, we have to find a bijection $\bar{\sigma}$ between $\mathcal{A} := \mathcal{S}_{2p} \setminus (\mathcal{X} \cup \{g^\ell, (2g)^\ell\})$ and $\mathcal{B} := \mathcal{S}_{2p} \setminus \{\frac{1}{2}(p-1), p-1, \frac{3}{2}(p-1), 2p-2, 2p-1, 2p\}$ such that

$$\{a^{\bar{\sigma}(a)}\}_{a \in \mathcal{A}} \sim_p \mathcal{A}$$

In particular we have

$$\mathcal{A} \sim_p \left\{ \underbrace{g^q, g^{q^2}, \dots, g^{q^{\ell-1}}, g^{(2q)}, g^{(2q)^2}, \dots, g^{(2q)^{\ell-1}}}_{2 \text{ times}} \right\}$$

and

$$\mathcal{B} \sim_{p-1} \left\{ \underbrace{q, q^2, \dots, q^{\ell-1}, (2q), (2q)^2, \dots, (2q)^{\ell-1}}_{2 \text{ times}} \right\}$$

Then it's enough to choose $\bar{\sigma}\left(g^{(\varepsilon q)^i}\right) = (\varepsilon q)^{i+\lfloor \frac{2i}{\ell+1} \rfloor}$ for all $i \in \mathcal{S}_{2p}$ and $\varepsilon \in \{1, 2\}$. That's straightforward to verify that this construction really works.

6. CONCLUSIONS

According to Theorems 1 and 2, if a integer $n \geq 2$ belongs to \mathbb{M} then $v_2(n) = 1$, $\frac{1}{2}n \in \mathbb{P}$, $\mu^2(\frac{1}{2}n - 1) = 1$ and $\frac{1}{2}n \notin (2\mathbb{S} + 1) \cup \{1, 3\}$. In particular, if such a integer exists, then $n \geq 62$. Once defined \mathbb{P}_{sf} the subset of \mathbb{P} such that $p \in \mathbb{P}_{\text{sf}}$ if and only $\mu^2(p - 1) = 1$, we deduce that $\mathbb{M} \cap [1, x] \subseteq \mathbb{P}_{\text{sf}} \cap [1, x/2]$ for all $x \geq 2$. Relying on Prime Number Theorem [1] and following a standard approach with Abel summation as in [10], it can be easily proved that there exists a positive constant A such that

$$\mathbb{P}_{\text{sf}} \cap [1, x] = \alpha \frac{x}{\ln x} + \mathcal{O}\left(\frac{x}{\ln^A x}\right)$$

where $\alpha := \prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p(p-1)}\right) \approx 0.37395$ is the Artin constant [4]. It follows that

$$|\mathbb{M} \cap [1, x]| \leq |\mathbb{P}_{\text{sf}} \cap [1, x/2]| \leq \frac{x}{5 \ln x} \text{ with } x \rightarrow \infty$$

Hence we proved that there exist at most $\frac{x}{5 \ln x}$ integers n in $\mathbb{N} \cap [2, x]$ such that our Conjecture does not hold, as far as x is sufficiently large.

It's remarkable that just a couple of years ago F. Liu proved in [7] that $|\mathbb{S}| = \infty$, solving the well known open problem about the infinitude of Sophie Germain primes. Incidentally, it proves that there exist infinitely many exponential numbers. A heuristic estimate for $|\mathbb{S} \cap [1, x]|$ is $2C_2 x / (\ln x)^2$, where $C_2 \approx 0.66016$ represents the twin prime constant [3]; although this estimate (due to G.H. Hardy and J.E. Littlewood) gives accurate prediction, it seems extremely difficult to prove rigorously in analytic number theory.

7. ACKNOWLEDGEMENTS

The author is grateful to Salvatore TRINGALI (Université Pierre et Marie Curie) and Carlo FIORITO DE FALCO (Università Bocconi) for suggesting remarks that improved the readability of the article.

REFERENCES

- [1] Apostol T.M., *Introduction to Analytic Number Theory*, New York: Springer-Verlag, 1976.
- [2] Bourbaki N., *Theory of Sets*, Théorie des Ensembles, 1970.
- [3] Caldwell C.K., *A amazing prime heuristic*, 2000.
- [4] Crandall R. and C. Pomerance, *Prime Numbers: A Computational Perspective*, Springer, Berlin, 2001.
- [5] Hardy G.H. and E.M. Wright, *An Introduction to the Theory of Numbers*, 6th edition, revised by D.R. Heath-Brown and J.H. Silverman, Oxford University Press, 2008.
- [6] Landau E., *Vorlesungen über Zahlentheorie*, Vol.2, Leipzig, 1927.
- [7] Liu F., *On the Sophie Germain prime conjecture*, Wseas Transactions on Mathematics, Vol.10, 2011.
- [8] Mollin R.A., *Algebraic Number Theory*, 2nd edition, Discrete Mathematics and Its Applications, Chapman and Hall/CRC, 2011.
- [9] Nagell T., *Introduction to Number Theory*, New York: Wiley, 1951.
- [10] Pappalardi F., F. Saidak and I.E. Shparlinski, *Square-free values of the Carmichael function*, Journal of Number Theory, 103, 2003.

UNIVERSITÀ BOCCONI, VIA SARFATTI 25, 20100 MILANO, ITALY.

E-mail address: leonetti.paolo@gmail.com